(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number
WO 01/31597 A1

(51) International Patent Classification[7]: G07F 9/00

(21) International Application Number: PCT/AU00/01324

(22) International Filing Date: 27 October 2000 (27.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 3712 28 October 1999 (28.10.1999) AU

(71) Applicant *(for all designated States except US)*: **GARAMEX PTY LTD** [AU/AU]; 1st Floor, 196 Stacey Street, Bankstown, New South Wales 2200 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WILSON, Steven, Paul** [AU/AU]; 7 Tagu Place, Kings Park, New South Wales 2148 (AU).

(74) Agents: **DAVIDSON, Geoffrey, Robert** et al.; Halford & Co. Level 7, 1 Market Street, Sydney, New South Wales 2000 (AU).

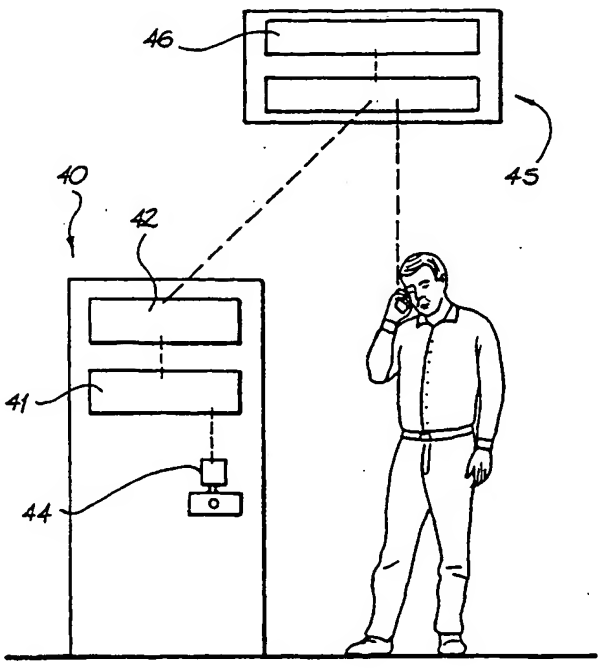
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: VENDING MACHINE SECURITY



(57) Abstract: A vending machine (40) with a modified security arrangement is disclosed. The vending machine (40) has a mechanical lock operated by an attendant and an electronic lock that is unlocked in response to a signal received from a remote monitoring station (45) with which the vending machine communicates. The attendant identifies themselves to the remote monitoring station by a wireless communication either directly or through the vending machine. The remote station verifies the attendant and sends a signal to the vending machine to unlock the electronic lock.

WO 01/31597 A1

VENDING MACHINE SECURITY

BACKGROUND OF THE INVENTION

The invention is described in the following statement:

The invention described herein relates to vending machines and more particularly to security systems for vending machines.

Vending machines are, by their nature, located in public places and therefore must be sufficiently secure to prevent unauthorised persons from breaking into them. However, these security systems must also be convenient enough to allow ready access to authorised persons for operations such as re-stocking, emptying the cash box, maintenance etc. Each service attendant will typically have responsibility for a large number of machines at various locations. As such, there is generally one master key that can service all locking devices for a controlled group of vending machines. This is a security risk if the key becomes lost or stolen.

SUMMARY OF THE INVENTION

In one form the present invention resides in a vending machine security arrangement including a vending machine including means for communication with a remote station, a mechanically operated locking mechanism operated by an attendant and an electronically operated locking mechanism, said remote station including means for receiving attendant identification from said attendant through wireless communication means and vending machine identification information, means for verifying said information and means for transmitting a signal to said vending machine to cause unlocking of said electronically activated locking mechanism.

In one embodiment the electrically operated locking mechanism acts on the mechanical mechanism so as to prevent the mechanical mechanism being opened until said unlocking signal is received from the remote station.

Preferably the security arrangement includes means for conducting an audit of the vending machine prior to unlocking of the electronically activated locking mechanism. More preferably, the audit information is transmitted from the vending machine to the remote station after which the remote station transmits the signal to the vending machine to cause unlocking of the electronic locking mechanism.

Still preferably, the host computer maintains a log of access to the vending machine including attendant identification and the time of access.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be further described with reference to preferred embodiments and to the accompanying figures, in which:

Fig. 1 is a schematic partial elevational cross section of a locking arrangement for a vending machine door in the locked position.

Fig. 2 is a schematic cross section of the locking arrangement modified according to the present invention when unlocked; and

Fig. 3 is a schematic depiction of the communications and control system operating the electrically operated locking mechanism.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figures 1 and 2 show a locking arrangement for a vending machine, in particular a vending machine incorporating a temperature control unit. In temperature controlled vending machines the lock performs two functions. The first obvious function is to

secure the door in a closed position to prevent access to the inside of the vending machine by unauthorised persons. The second function is to ensure that the vending machine is properly sealed in order that the temperature control unit can operate most efficiently. To this end, as shown in Figures 1 and 2 a conventional mechanical locking mechanism for a vending machine includes a generally T-shaped bar 10 having a stem 13 with a lower threaded portion 11, a rectangular locking plate 12, and an outwardly spring loaded locking pin 16 operated by a conventional key lock 17. The threaded stem 11 engages a locking nut 14 fixed within the vending machine. The T-shaped bar 10 is received through an aperture extending through the door of the vending machine. To secure the door closed, the T-bar 10 is inserted through the door aperture until the threaded stem 11 engages the locking nut 14. The locking plate 12 is used as a handle to wind the threaded stem 11 through the nut 14 thereby securing the door in a closed and sealed position. As a final securing step, the locking plate 14 is pressed inwards against the actions of a spring 15 until the plate 14 is substantially flush with the vending machine door. At this point the locking pin 16 previously withdrawn into an upper portion of the stem 13 pops out and engages the door, thus securing the T-bar with the locking plate flush with the door. The locking plate is rectangular or otherwise non-circular and fits within a corresponding recess in the door face.

To re-open the door, the locking pin 16 is disengaged through actuation of the key lock 17 in conventional manner. Once the pin 16 has been withdrawn, the spring 15 acts to eject the plate 14 outwards from the door so that it can be used as a handle for unscrewing the threaded stem 11 from the nut 14.

The conventional, mechanical lock mechanism as described above forms part of the illustrated vending machine security system according to the invention. To this is retro-fitted a second locking mechanism as described below, to adapt the arrangement in accordance with the present invention.

A solenoid-operated locking pin arrangement 30 is mounted to the interior of the vending machine, including a solenoid 31 and a pin 32 biased by a spring 33 to its

extended position in which opening of said vending machine is prevented. The locking arrangement 30 works by charging the solenoid 31 creating an electro-magnet that withdraws the pin 32 from its extended position so that the vending machine may be opened.

The location of the solenoid locking pin arrangement 30 within the vending machine is arbitrary provided that it is situated so as to prevent opening of the vending machine door even if the mechanical lock has been unlocked. The location will depend on the construction of the vending machine and whether the locking mechanism is being designed into a new vending machine or is being retro-fitted to an existing vending machine. Other factors that may influence the location of the electronic locking arrangement 30 include the proximity of other metal components that may become magnetised as the solenoid 31 is charged thereby preventing proper movement of the pin 32.

In one embodiment as shown in Figs. 1 and 2 the above mentioned T-bar 10 is modified to include a radial bore 34 extending across a diameter of an upper portion of the stem 13 and sized to receive the pin 32. When the door of the vending machine is closed with the T-bar 10 received in the locking position, the bore 34 and pin 32 align such that the pin 32 is biased under the influence of the spring 33 to penetrate into the bore 34. Therefore when the door of the vending machine is closed and secured by the first locking mechanism, the second locking mechanism is also engaged and prevents removal of the T-bar 10 even if an authorised attendant activates the locking pin 16 through the key lock 17.

As shown in Fig. 3, a vending machine 40 includes a micro-processor 41 and a communication interface 42 for communication between the micro-processor 41 and a remote monitoring station 45, e.g. a host computer. The communication may be via a hard wired telephone network but is preferably effected through an existing GSM network or other wireless communication. The monitoring station 45 may service a plurality of vending machines, and includes a database 46 containing identification codes for all vending machines controlled by the monitoring station 45 and codes for

all attendants authorised to service those machines. The manner in which the remote station interfaces with the vending machine is not relevant to the present invention and may be in any known manner. Most simply the vending machine 40 may include a receiver that receives a signal to unlock the electronic lock 44 and then charges the solenoid 31. Alternatively the vending machine 40 and remote station 45 may interface using the standard DEX UCS protocol in common use for conducting vending machine audits or in a manner described in our co-pending application titled "Vending Machine Communications", the contents of which are incorporated herein by reference.

In one preferred embodiment the remote monitoring station includes a further communications interface, allowing an attendant to contact the monitoring station via GSM telephone or similar and enter machine and attendant identification security codes. Upon verification of the attendant's authorisation to open the vending machine, the monitoring station opens an active communications link to the vending machine's communications interface. The remote station then instructs the vending machine's micro-processor to conduct an audit of the vending machine's contents which is achieved by the micro-processor recording the values of the various registers of the vending machine such as the cash box register and the many product registers for the different products dispensed by the vending machine. The micro-processor then transmits the values of the registers to the remote station which records this information together with a log of the attendant's access to the machine. Once the audit has been completed, the remote station then instructs the micro-processor to unlock the electronic locking mechanism.

The vending machine then utilises the vending machine's LED or other display to inform the attendant when the audit and electronic unlocking is completed and is ready for key unlocking.

In an alternative embodiment, communications between the attendant and the remote station all occur through the vending machine. In this embodiment the attendant carries an encoded key, such as a magnetically encoded swipe card or a radio

transmitting key, encoded with an attendant identification code. The vending machine includes a corresponding device for reading or receiving the attendant identification codes such as a card reader or radio receiver. The attendant provides their code to the vending machine which then initiates a wireless communication link to the remote station and transmits both a vending machine identification code and the attendant identification code. Communication costs for this embodiment are generally less compared to the embodiment described above as only one communication link to the remote station is required. The drawback is that the vending machine requires more intelligence both to receive the attendant identification code and to initiate a communication to the remote station.

Once the attendant has completed the required tasks, the vending machine is closed by inserting the T-bar in the manner described above. The vending machine senses when the T-bar is securely in the locking position and uncharges the solenoid 33 causing the pin 32 to re-engage the T-bar 10 or other part of the vending machine. The monitoring station may again perform an audit if necessary, before breaking the communications link to the vending machine.

The vending machine may include a time-out that automatically relocks the electronic lock in the event that the vending machine is not opened by the attendant within a predetermined time, e.g. 2 minutes, after electronic unlocking.

To reduce communication costs, the vending machine stores an accepted or verified attendant identification code for a predetermined period eg. 30 minutes. In this way, an attendant can return to a machine and re-open it to complete a task without the need to re-establish a communications link between the vending machine and the remote station.

Similarly, the vending machine may store a denied request attendant code for a predetermined period, eg. 30 minutes, to prevent the machine from establishing a communication link to the remote station in the event that a denied request to access the machine is subsequently repeated.

The security arrangement of the present invention may also include facility for sensing the time for which the machine door has been open and, after a predetermined time exceeding the usual service requirement, for example 30 minutes, sending an alarm signal to the remote monitoring station.

An advantage of the illustrated arrangement is that it provides a convenient combination of mechanical and electronically controlled locking, easily retro-fitted to the existing locking mechanism of a vending machine.

The security arrangement of the present invention provides additional security because if an attendant's mechanical key is lost or stolen, unauthorised parties cannot gain access to the vending machine due to the electronic lock. If an attendant's encoded key is lost or stolen, the attendant can report this to a system administrator who can remove the key code of the lost key from a list of codes acceptable to the host computer so that a person attempting to gain access to a vending machine using the lost encoded key will be denied. This is also true for a system where an attendant contacts the host computer directly, for example using a mobile telephone, to provide their identification. If an unauthorised person has obtained an attendant's identification codes, the attendant can report those codes to have them removed from the list of codes acceptable by the host computer.

A further security advantage arises because it is possible to conduct an audit of the vending machine immediately before and immediately after the vending machine has been accessed by an attendant. Therefore any unscrupulous action by the attendant, eg theft of cash box money or stock, will quickly come to the attention of the system administrator or vending machine owner.

While particular embodiments of this invention have been described, it will be evident to those skilled in the art that the present invention may be embodied in other specific forms without departing from the essential characteristics thereof. The present embodiments and examples are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims

rather than the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

CLAIMS

1. A vending machine security arrangement including a vending machine including means for communication with a remote station, a mechanically operated locking mechanism operated by an attendant and an electronically operated locking mechanism, said remote station including means for receiving attendant identification from said attendant through wireless communication means and vending machine identification information, means for verifying said information and means for transmitting a signal to said vending machine to cause unlocking of said electronically activated locking mechanism.

2. A security arrangement according to claim 1 further including means for conducting an audit of said vending machine prior to unlocking of said electronically activated locking mechanism.

3. A security arrangement according to claim 1 wherein said remote station includes means for receiving attendant identification information and vending machine identification information directly from said attendant through wireless communications means and means for initiating communications with the vending machine identified by said vending machine identification information.

4. A security arrangement according to claim 1 wherein said vending machine further includes means for receiving attendant identification information from said attendant and means for transmitting said attendant identification information and vending machine identification information to said remote station.

5. A security arrangement according to claim 4 wherein said vending machine initiates communication with said remote station in response to receiving attendant identification information from an attendant.

6. A security arrangement according to claim 4 wherein said vending machine stores verified attendant identification information for a predetermined period after unlocking said electronic locking mechanism.

7. A security arrangement according to claim 4 wherein said vending machine stores denied attendant identification information for a predetermined period after said attendant identification information is transmitted to said remote station.

8. A security arrangement according to claim 1 wherein said electronically activated locking mechanism includes a solenoid and a pin moveable between a locking position in which access to said vending machine is prevented and an unlocking position and wherein said solenoid is charged to cause said pin to move from its locking position to its unlocking position in response to said vending machine receiving said signal from said remote station.

9. A vending machine including a mechanically operated locking mechanism operated by an attendant, an electronically activated locking mechanism, wireless communication means for communicating with a remote station, means for receiving attendant identification information from an attendant, means for transmitting said attendant identification information and vending machine identification information to said remote station and means for unlocking said electronically activated locking mechanism in response to a signal received from said remote station that said attendant is authorised to access said vending machine.

10. A vending machine according to claim 9 further including means for conducting an audit of said vending machine prior to unlocking of said electronically activated locking mechanism.

11. A vending machine according to claim 10 further including means for transmitting audit information to said remote station.

12. A vending machine according to claim 9 wherein said vending machine initiates communication with said remote station in response to receiving attendant identification information from an attendant.

13. A vending machine according to claim 9 wherein said vending machine stores verified attendant identification information for a predetermined period after unlocking said electronic locking mechanism.

14. A vending machine according to claim 4 wherein said vending machine stores denied attendant identification information for a predetermined period after said attendant identification information is transmitted to said remote station.

15. A vending machine according to claim 9 wherein said electronically activated locking mechanism includes a solenoid and a pin moveable between a locking position in which access to said vending machine is prevented and an unlocking position and wherein said solenoid is charged to cause said pin to move from its locking position to its unlocking position in response to said signal being received from said remote station.

16. A vending machine according to claim 9 wherein said electronically activated locking mechanism acts on said mechanical locking mechanism such that unlocking of said mechanical locking mechanism is prevented prior to unlocking of said electronically activated locking mechanism.

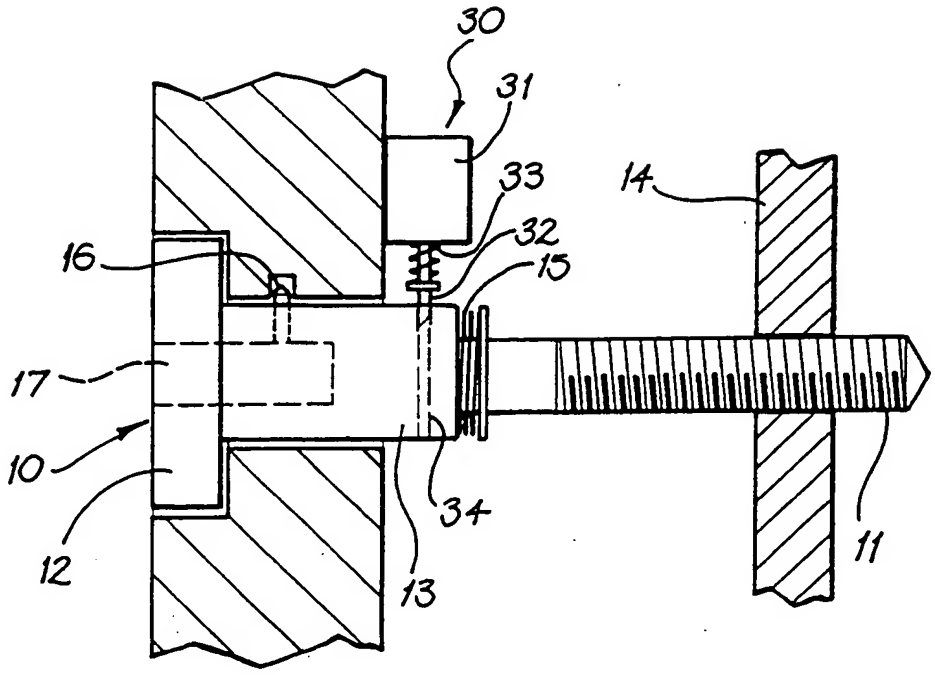


FIG. 1

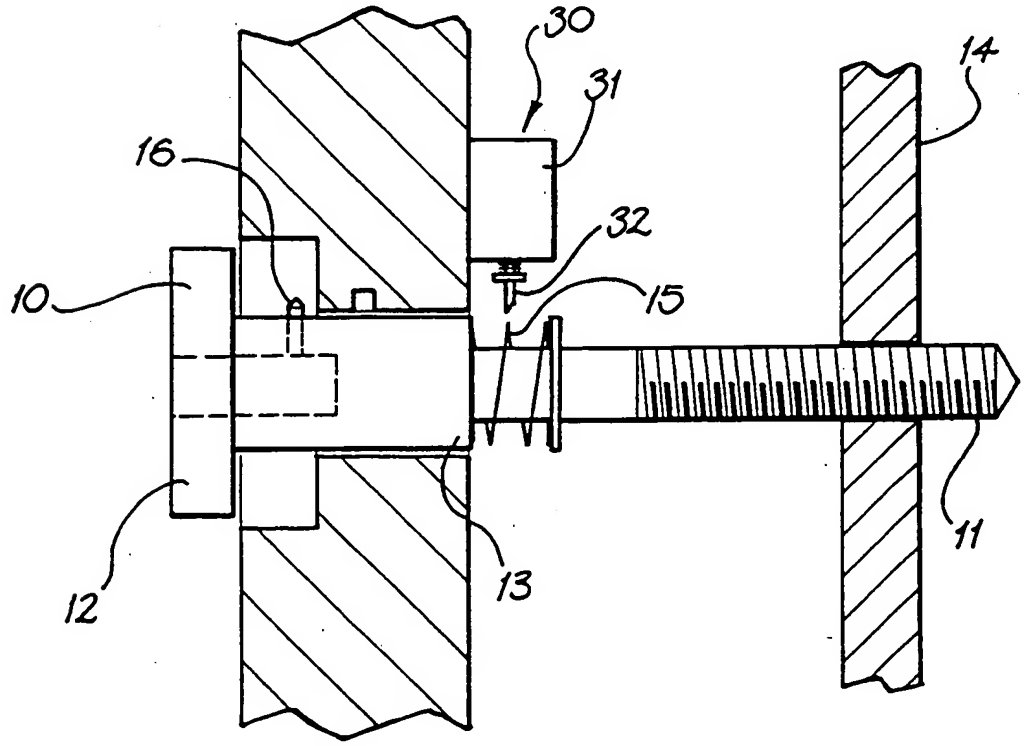


FIG. 2

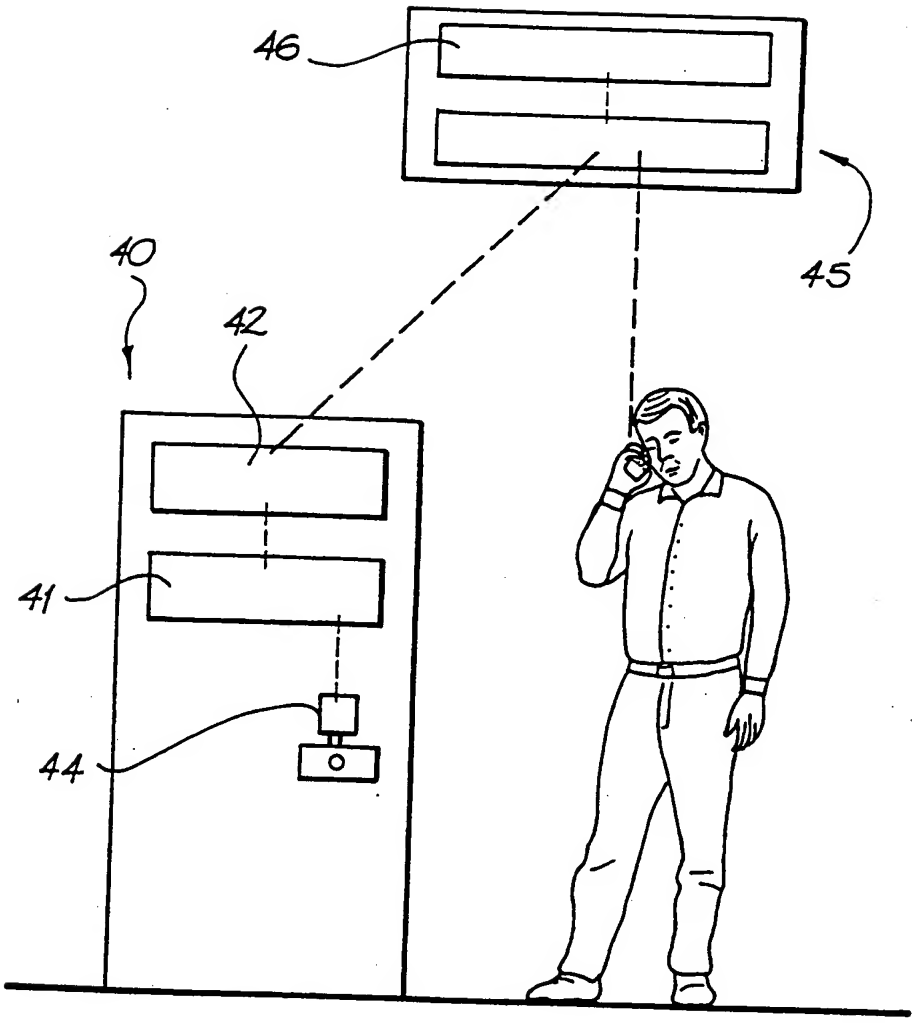


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU00/01324

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G07F 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPAT (lock, electronic, vending)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	AU-A-55542/99 (Stillwagon) 24 February 2000 Whole document	1
Y	US 5 947 328 (Kovens et al.) 7 September 1999 Abstract, column 13, lines 30-62	1,2,9-11
Y	US 5 930 771 (Stapp) 27 July 1999 Abstract, columns 1 to 4	1,2,9-11

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 2000	5 - DEC 2000 5 - DEC 2000

Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	DALE E. SIVER Telephone No : (02) 6283 2196

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU00/01324

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 94/21089 (Medeco Security Locks, Inc.) 15 September 1994 Whole document	1,2,9-11,15,16
Y	US 5 091 713 (Horne et al.) 25 February 1992 Abstract,figures, column 7 lines 29-51	1,2,9-11
A	WO 97/28510 (Imaging Technologies) 7 August 1997 Abstract, figures 12a to 13e	1,2,9-11

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU00/01324

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
AU	55542/99	WO	2000/09838				
US	5947328	CA	2232908	US	6050447		
US	5930771	NO	MEMBERS				
WO	94/21089	CA	2157480	EP	688491		
US	5091713	NO	MEMBERS				
WO	97/28510	AU	15838/97	AU	7871/96	AU	4063/96
		JP	2000504447	EP	956544		

END OF ANNEX